ÖSTERMALM
FOND & FÖRSÄKRING

Policy enligt lagkrav: Hantering av personuppgifter enligt GDPR

Dokumentet har upprättats och antagits av styrelsen för OMFF AB.

1. Allmänt

Med "Bolaget" avses i detta dokument OMFF AB.

1.1 Bakgrund

Enligt artikel 8.1 i Europeiska unionens stadga om de grundläggande rättigheterna (2010/C 83/02) och artikel 16.1 i Fördraget om Europeiska unionen och fördraget om Europeiska unionens funktionssätt 2012/C 326/01 har varje fysisk persons rätt till skydd för dennes personuppgifter. Dessa uppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund.

Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (GDPR) har byggts upp som en förbudslag, d.v.s. utan stöd i lag är behandling ej tillåten. Förordningen har utformats till skydd för den personliga integriteten när det gäller hantering och behandling av personuppgifter. Förordningen kompletteras av lag med kompletterande bestämmelser till EU:s dataskyddsförordning och förordning med kompletterande bestämmelser till EU:s dataskyddsförordning samt artikel 29-gruppens vägledning.

Ansvaret för behandlingen av personuppgifter åläggs den som behandlar sådana uppgifter samt att det sker på ett lagligt sätt. I sammanhanget bör förtydligas att GDPR är subsidiär i förhållande till lagar på nationell nivå, vilket innebär att annan lag gäller framför GDPR.

Begreppet "behandlar" är brett och det omfattar bl.a. insamling, registrering, lagring, bearbetning, spridning, med mera. GDPR är en förordning som är gällande direkt i hela EU vilket underlätta flödet av information EU-länderna emellan.

1.2 Syfte

GDPR har till syfte att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter. Förevarande policy, samt Riktlinjer för efterlevnad GDPR bilagt till förevarande policy, har upprättats inom Bolaget för att i möjligaste mån undvika att personuppgifter behandlas felaktigt. Den behandling som företas ska vara förenlig med GDPR. Innan en personuppgiftsansvarig ska behandla uppgifter måste denna klart och tydligt ha ett bestämt syfte med behandlingen, t.ex. lönehantering, provisions/ersättningshantering, personaladministration eller besökskontroll.

2. Personuppgifter

All information som kan härledas direkt eller indirekt till en fysisk person som är i livet utgör personuppgifter. Även uppgift om en avliden släkting kan vara en personuppgift om uppgiften anknyter till en levande person, men i normalfallet inte. Endast uppgift om t.ex. en persons födelsedatum utgör inte en personuppgift. Skulle det däremot röra sig om ett personnummer

betraktas det i allra högsta grad som en personuppgift. Uppgiften ska således leda till en identifiering/spårbarhet.

GDPR tar sikte på sådan behandling av personuppgifter som helt eller delvis görs med hjälp av datorer. Även annan behandling av uppgifter som kan vara tillgängliga för sökning eller sammanställning enligt särskilda kriterier (s.k. manuellt register) omfattas av lagen.

GDPR gäller dock inte för behandling av personuppgifter som en fysisk person utför som ett led i en verksamhet av rent privat natur, t.ex. upprätta en elektronisk dagbok eller föra ett register över sina vänners adresser och telefonnummer.

2.1 Behandling av personuppgifter

Bolaget ska endast behandla personuppgifter som är nödvändiga, relevanta och ändamålsenliga. Behandlingen ska genomsyras av laglighet, korrekthet och öppenhet. Personuppgifterna ska således vara korrekta och om nödvändigt uppdaterade. Rimliga åtgärder ska vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål. För att en behandling ska anses som laglig ska exempelvis något av följande vara uppfyllt, se även Bilaga 1:

- Behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås.

- Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar Bolaget.

- Den registrerade har lämnat sitt samtycke till att dennes personuppgifter behandlas för ett eller flera specifika ändamål.

Bolagets ska alltid använda sig, vid personuppgiftbehandlingen, av ändamålsbegränsning. Personuppgifterna får aldrig behandlas på ett sätt som är oförenligt med dessa ändamål. Bolaget ska även alltid ha den registrerades integritet i fokus i sitt arbete. All personuppgiftsbehandling ska ske på ett strukturerat sätt.

2.2 Registerföring

Bolaget, och i tillämpliga fall dennes personuppgiftsbiträde, ska föra ett register över personuppgiftsbehandlingen som utförts under dennes ansvar.

Registret ska innehålla:

- kontaktuppgifter till Bolaget, dennes personuppgiftsbiträde samt dataskyddsombud,
- ändamålen med personuppgiftsbehandlingen,
- en beskrivning av kategorierna av registrerade och kategorierna av personuppgifter, och
- kategorierna av mottagare till vilka personuppgifter lämnats, eller ska lämnas, ut.

Bolaget ska även, om möjligt, notera förutsedda tidsfrister för radering av de olika kategorierna av uppgifter samt allmänt beskriva de tekniska och organisatoriska säkerhetsåtgärderna som utförts med anledning av de registrerade personernas rättigheter och friheter.

3. Personuppgiftsansvarig och dataskyddsombud samt personuppgiftsbiträde

Bolaget är att betrakta som personuppgiftsansvarig i sin verksamhet och bestämmer vilka uppgifter som ska behandlas och vad de ska användas till. Den personuppgiftsansvarige är skyldig att föra ett register över de behandlingar som görs inom bolaget och att till Datainspektionen anmäla personuppgiftsincidenter. Om Bolaget har utsett ett dataskyddsombud ska ombudet se till att personuppgifterna behandlas korrekt. Det är fortfarande personuppgiftsansvarig som har det slutliga ansvaret för behandlingen.

Sven-Arne Sjödin, sas@omff.se, är utsedd som OMFF´s dataskyddsombud.

Ett ombud har till uppgift att stötta och hjälpa den personuppgiftsansvariga att följa lagens uppställda krav och därigenom skapa bättre förutsättning för att minska riskerna för fel och därigenom skadeståndskrav och andra externa kostnader som kan åläggas den personuppgiftsansvarige. Ombudet har även till uppgift att kontrollera att den personuppgiftsansvarige följer lagens krav. Kontrollen ska utföras kontinuerligt och anpassas till den verksamhet Bolaget bedriver.

I de fall Bolaget använder sig av ett Personuppgiftsbiträde - som ska behandla personuppgifter för en personuppgiftsansvarigs räkning - ska ett skriftligt avtal upprättas, ett s.k. personuppgiftsbiträdesavtal.

4. Förpliktelser mot den behandlade

Bolaget har vid begäran från den behandlade en skyldighet att:

- utge information om alla personuppgifter som den personuppgiftsansvariga har lagrat om den behandlade,
- rätta personuppgifter som är fel och komplettera med sådana personuppgifter som saknas och som är relevanta med hänsyn till ändamålet med personuppgiftsbehandlingen,

• radera personuppgifter som avser den behandlade om uppgifterna inte längre behövs för de ändamål som de samlades in för eller för att uppfylla en rättslig förpliktelse,

• begränsa behandlingen av personuppgifter avseende den behandlade till vissa avgränsade syften,

• underlätta överflyttning av personuppgifter om det är den behandlade själv som har lämnat uppgifterna och behandlingen sker med stöd av ett samtycke eller för att uppfylla ett avtal med den behandlade (dataportabilitet),

• ge kunden ett beslut av en person i stället för någon form av automatiserat beslutsfattande, inbegripet profilering om beslutet kan ha rättsliga följder för den enskilde eller på liknande sätt i betydande grad påverkar honom eller henne.

Sådan begäran görs skriftligen till Bolaget och ska vara undertecknad av kunden. Begäran ska bemötas inom en månad från det att Bolaget tog emot begäran. Bolagets ovan listade skyldigheter gäller i den mån dessa skyldigheter inte motsätter annan lag.

5. Bevarandet av personuppgifter

Bolaget ska ha som utgångspunkt att endast behålla personuppgifterna i den mån det är nödvändigt med hänsyn till de ändamål för vilka de samlades in. Bolaget ska endast behålla uppgifterna så länge det behövs för att kunna fullgöra vissa åtagande, t.ex. hantera klagomål, vara behjälplig i skadeärenden, med mera. Se även Bilaga 2.

6. Säkerhet

Bolaget ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas utifrån den tekniska lösning som används inom organisationen. Bolaget ska alltid ha kundens integritet i fokus och ska vid nya tekniska uppdateringar implementera och säkerställa kundens integritet.

6.1 Incidentrapportering

Med personuppgiftsincident menas en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats av Bolaget.

Bolaget har en skyldighet genom lag att anmäla personuppgiftsincidenter till Datainspektionen inom 72 timmar från och med att Bolaget fick kännedom om personuppgiftsincidentet i det fall personuppgiftsincidenten sannolikt kan leda till en hög risk för fysiska personers rättigheter och friheter. Om den Bolaget inte lyckas anmäla personuppgiftsincidenten inom 72 timmar ska den personuppgiftsansvarige motivera orsaken till förseningen.

Anmälan om personuppgiftsincident ska innehålla följande:

1. personuppgiftsincidentens art, inbegripet, om så är möjligt, de kategorier av och det ungefärliga antalet registrerade som berörs samt de kategorier av och det ungefärliga antalet personuppgiftsposter som berörs,

2. kontaktuppgifterna till Bolagets mest insatta gällande incidenten där mer information kan erhållas,

3. beskriva de sannolika konsekvenserna av personuppgiftsincidenten, och

4. beskriva de åtgärder som Bolaget har vidtagit eller föreslagit för att åtgärda personuppgiftsincidenten, inbegripet, när så är lämpligt, åtgärder för att mildra dess potentiella negativa effekter.

Bolaget ska dokumentera alla personuppgiftsincidenter, inbegripet omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits.

Om personuppgiftsincidenten sannolikt, med hög risk, skulle äventyra den fysiska personens rättigheter och friheter ska Bolaget utan onödigt dröjsmål informera den registrerade om personuppgiftsincidenten.

Informationen ska vara tydlig och klar och åtminstone innehålla de upplysningar och åtgärder som beskrivs ovan i punkt 2-4. Sådan information behöver dock inte lämnas om:

- dessa personuppgifter är oläsbara för personer som inte har behörighet att få tillgång till personuppgifterna, såsom vid kryptering,

- om Bolaget efter incidenten vidtagit åtgärder som säkerställt att den höga risk som tidigare bedömts inte längre sannorlikt kommer uppstå, eller

- om informationslämnandet skulle anses utgöra en oproportionell ansträngning, i sådant fall ska istället allmänheten informeras eller liknande åtgärd vidtas.

7. Ikraftträdande och fastställande

Dokumentet har upprättats och antagits av styrelsen för Bolaget som även tillhandahåller löpande uppdateringar av dokumentet. Senaste antagen version ersätter samtliga tidigare versioner. Dessa riktlinjer ska fastställas och godkännas av Bolagets styrelse minst en gång per år även om inga ändringar beslutas.